FACT SHEET

NSTISSP No. 12
National Information Assurance (IA) Policy for U.S. Space Systems

Background:

1. The National Security Telecommunications and Information Systems Security Committee (NSTISSC) has issued National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 12, Subject: *National Information Assurance (IA) Policy for U.S. Space Systems*.

2. The NSTISSC was established by National Security Directive (NSD) No. 42, dated July 1990, and is responsible for developing and promulgating national policies applicable to the security of national security telecommunications and information systems.

Introduction:

3. Presidential Decision Directive (PDD) No. 49, Subject: *National Space Policy*, dated 19 September 1996, has established that U.S. space activities are critical to the national security of the United States. Commercial space activities are also closely linked to the operation of the U.S. Government's critical infrastructures as identified in PDD No. 63, Subject: *Critical Infrastructure Protection*, dated 22 May 1998, and may, on occasion, be leveraged to satisfy national security requirements. Based on their importance, it is imperative that a comprehensive, national-level IA space policy be developed, promulgated, and adopted that will ensure the confidentiality, authenticity, integrity, availability, and survivability of associated communications and communications

networks under a wide range of peace- or war-time cyber threat scenarios.

4. The primary objective of NSTISSP No. 12 is to ensure that IA is factored into the planning, design, launch, sustained operation, and deactivation of all U.S. space systems used to collect, generate, process, store, display, or transmit/receive national security information, as well as any supporting or related national security systems. The policy also serves to remind users of space assets outside the national security community that they may wish to factor IA into those space activities associated with the operation and/or maintenance of critical U.S. infrastructures.

Scope:

5. NSTISSP No. 12 applies to:

a. All U.S. Government or commercially owned and operated space systems (i.e., U.S. space systems) used to collect, generate, process, store, display, or transmit/receive national security information.

b. All supporting or related national security systems.

c. All U.S. Government Departments and Agencies involved in acquisition, launch, operation, maintenance, or lease of these same systems.

Policy:

6. U.S. Space systems are critical to the defense of the nation and are important components of its critical infrastructures.

7. The successful launch and operation of U.S. space systems must be based on the application and integration of a combination of IA products, services, measures, and techniques that provide acceptable or desired levels of assurance for both information and associated information systems and networks. The following requirements must be addressed in a balanced manner:

a. Confidentiality, i.e., assuring that information is not disclosed to unauthorized persons, processes, or devices.

b. Authentication, i.e., establishing the validity of a transmission, message, or originator, or as a means of verifying an individual's authorization to receive specific categories of information.

c. Data Integrity, i.e., ensuring that data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

d. Availability, i.e., ensuring timely and reliable (on demand) access to data and information services for authorized users.

e. Non-repudiation, i.e., assuring the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

f. Personnel security and the physical security of communication security (COMSEC) and IA products and their associated keying materials.

8. Designers, developers, planners, and end users of U.S. space systems shall ensure that IA requirements are considered and addressed during the entire life-cycle of all U.S. space systems, as well as all supporting or related national security systems. "Life-cycle" includes all stages of planning, design, research and development, test and evaluation, deployment, operations, product improvement, and system retirement.

9. Data owners, platform owners, launch operators, and mission operators shall identify IA requirements and acquire and implement those products, services, measures, or techniques necessary for providing the desired or required levels of assurance.

10. The following IA requirements shall be addressed and satisfied for U.S. space systems:

a. Approved U.S. cryptographies* shall be used to provide confidentiality for:

1). The command/control up-links.

2). The data links used to transmit national security information between the ground and space platforms.

3). The cross-links between space platforms.

4). The downlinks from space platforms to mission ground or processing centers.

b. Supporting or related national security systems will be similarly protected.

c. A Secure Command Destruct System (SCDS) shall be required for all launch vehicles. This requirement applies to both U.S. Government and U.S. commercial launch vehicles, which may be used to launch U.S. space platforms.

* Approved U.S. Cryptographies: Hardware, firmware, or software implementations of algorithms which have been reviewed and approved by the National Security Agency (NSA), the purposes of which are to provide authentication or confidentiality for national security information or systems.

d. A Cryptographic Security Plan (CSP) shall be required for the launch of all U.S. space systems incorporating approved U.S. cryptographies.

e. Approved U.S. cryptographies shall be required for use on commercial imagery satellites where there is either foreknowledge or a reasonable expectation (based on documented U.S. planning or strategies), that such platforms may, during periods of international crises or wartime hostilities, be used to satisfy national security requirements involving classified information, or information determined to be critical or essential to the operational or organizational missions of U.S. Government entities.

f. Subject to policy and guidance for non-national security information and systems, U.S. Government Departments and Agencies may wish to consider the IA requirements of this policy for those space systems that may be critical or essential to the conduct of organizational missions, or for information or systems which may be associated with the operation of critical infrastructures.

Responsibilities:

11. The Director National Security Agency (DIRNSA) shall:

a. Review and approved all cryptographies intended to satisfy the IA requirements associated with this policy.

b. Provide IA advice and assistance to U.S. Government Departments and Agencies.

c. Review and approve all CSPs prior to the launch of U.S. or foreign space systems incorporating approved U.S. cryptographies.

d. Establish and maintain a database of all U.S. and foreign space systems which employ approved U.S. cryptographies.

12. Heads of U.S. Government Departments and Agencies shall:

a. Ensure compliance with the IA requirements of this policy for the acquisition, launch, operation, and maintenance of all U.S. space systems used to collect, generate, transmit, process, store, or display national security information, as well as for any related national security systems. Compliance includes:

1). Programming those funds required to acquire IA products, services, measures or techniques.

2). Ensuring that IA products, services, and measures are integrated, activated and sustained as critical security components of all U.S. space systems.

b. Ensure, through licensing or contractual relationships, that the requirements of this policy are imposed on those U.S. or foreign commercial entities involved in the launch, operation or maintenance of U.S. space systems.

c. Determine whether this policy should be applied to those space systems under their control, purview or cognizance that may be directly related to the operation and maintenance of critical U.S. infrastructures.

Qualifications and Exceptions:

13. This policy establishes minimum requirements for providing IA for U.S. space systems. Heads of U.S. Government Departments and Agencies may impose more stringent requirements on the operation of their systems.

14. The SCDS requirements of this policy do not apply to the commercial launch of commercial satellites that do not use approved U.S. cryptographies nor are ever intended to provide support to, or be part of a national security system.

15. Exceptions to this policy may be granted by the NSTISSC on a case-by-case basis.

Questions:

16. Any questions on this Policy Fact Sheet should be referred to the NSTISSC Secretariat @ (410) 854-6805 or email nstissc@radium.ncsc.mil.